國防安全雙週報

第 91 期

臺北市博愛路 172 號

電話（02）2331-2360

傳真（02）2331-2361

2025 年 7 月 17 日發行

財團法人國防安全研究院

Institute for National Defense and Security Research

Contents

解放軍加速 AI 融合應用之評析

王綉雯

中共政軍與作戰概念研究所

焦點類別：解放軍、軍事科技、戰爭模式

壹、前言

今（2025）年6月24日，中國航空工業集團（Aviation Industry Corporation of China, AVIC）在北京召開人工智慧（Artificial Intelligence，中國稱人工智能，以下簡稱為 AI）大會。會中發佈了《全面加速人工智能技術發展和應用的決定》及《「人工智能+」專項三年行動方案》；同時成立該集團「人工智能專家諮詢委員會」、設立首批 AI 專業技術實驗室並任命首批 AI 專業技術領軍人才。此會議有多名中共國家部委、軍方機關及科研機構人士出席，該集團高階幹部表示將透過 AI 技術推動航空裝備朝智能化及實戰化轉型，打造「新域新質作戰力量」，以掌握未來戰場主動權。此外，中共多家重要軍工央企如：中國航天科技集團（China Aerospace Science and Technology Corporation, CASC）、中國船舶集團（China State Shipbuilding Corporation, CSSC）等也已通過設立「智能研究院」，加速研發無人系統及極音速武器等，以符合未來智能化作戰需求。[1]

貳、安全意涵

一、 中共加速AI軍事應用加劇地緣政治不安

AI 被視為改變遊戲規則（game-changing）的重大關鍵技術，目前是美中爭霸的重中之重。從俄烏戰爭及以巴衝突的諸多演示，如：分析衛星影像、找出地理定位、蒐集大量情報、識別及建立攻

[1] 〈中國航空工業集團召開人工智慧大會〉，《中國航空新聞網》，2025 年 6 月 24 日，https://www.cannews.com.cn/yaowen/2025/06-24/514znwKD.html；〈國防軍工行業觀察：航空工業集團召開人工智慧大會，板塊單日漲幅近 4%〉，《工業和信息化部工業文化發展中心》，2025 年 7 月 1 日，https://www.gxbxxpt.org.cn/news/detail?id=6267&m=news。

擊名單等，可窺見 AI 軍事應用將大幅改變戰爭型態。中共擁有全球僅次於美國的 AI 實力、民用無人機約 80%的全球市佔率、自主的北斗衛星導航系統和 5G 通訊技術、機器人的完整生產鏈等，有充足條件發展 AI 軍事應用。再加上其主要軍工集團正透過「軍民融合」政策加速 AI 在武器研製的應用（表 1），若能順利研發並量產如：滯空攻擊彈藥（loitering munition）、無人武器平台等低成本且精確攻擊之武器，將大幅提升解放軍作戰能力。對於在東海、台海、南海等區域和中國有領土或主權糾紛的國家而言，中共造成的安全威脅恐日益升高。

二、解放軍持續發展AI軍事應用場景及關鍵技術

AI 軍事應用的發展方向主要有八種，分別是：輔助作戰決策、態勢感知和目標識別、情報分析處理、無人武器平台、智慧武器裝備、電子戰及網路攻防、智慧後勤保障，以及增強單兵作戰效能等。目前基於 AI 技術之進展，應用場景主要是取代重複性勞動、快速處理大量訊息、在惡劣環境下作業等三大類。[2]

解放軍的「智能化戰爭」是以美軍為標竿，認知到 AI 是智能化作戰核心技術，且必須有強大的網絡做為支撐。解放軍對於運用 AI 的智能化作戰技術及能力十分重視，聚焦於態勢感知及情報融合、動態組網及通訊、智慧決策及控制、無人系統及蜂群作戰等。[3]然而，儘管解放軍在 2024 年實戰化訓練中，已驗證其智能化指揮系統可支持多軍種數據即時共享，但是距離需要軟體和硬體結合、虛擬和現實整合，且掌握大量數據的「智能化戰爭」作戰階段，似乎還有不小的差距。為此，中共軍工央企集團正加速融入 AI 應用場景和

[2] 陶銳、楊祖耀，〈人工智能技術軍事應用重點領域及成熟度評價研究〉，《指揮控制與模擬》，第 46 卷第 2 期，2024 年 4 月，頁 64-65。

[3] 孔光、王新等，〈智能化戰爭作戰體系前瞻〉，《軍事文摘》，第 10 期，2024 年，轉引自《中國指揮與控制學會》，2024 年 10 月 17 日，http://www.c2.org.cn/h-nd-1331.html。

發展關鍵技術，並以航天（太空）、航空、船舶（海洋）三大領域為優先。

參、趨勢研判

一、中共將加速AI軍事應用之「軍民融合」

前述四大智能化作戰技術（態勢感知及情報融合、動態組網及通訊、智慧決策及控制、無人系統及蜂群作戰），傳統軍工集團難以自行研發，勢必將加速吸納民間企業的 AI 產品和人才。以今年 5 月在北京舉辦的軍事博覽會來看，參展民間企業達 500 多家，提出 3,000 多項產品及解決方案，其中，民間企業提出的 AI 大模型軍事應用，包括：智慧化指揮控制系統、輔助軍事訓練模型、軍事決策大語言模型、作戰模擬推演系統等，[4]而年初橫空出世的DeepSeek大語言模型也已被用於解放軍附屬醫院體系。[5]民間企業在軍用AI領域的研發創新能量，將成為解放軍智能化作戰能力的重要基礎。

這些研發軍用 AI 的民間企業多為新創公司，中共軍工央企早已利用創投方式參與其早期投資，或以參股、併購等「混合所有制」方式加以吸納。然而，傳統軍工集團和 AI 新創公司之間的磨合仍需時間。例如：新創公司規模小，內部管理結構較平等，容許研發人員嘗試錯誤，且能快速因應環境做出調整。傳統軍工集團則規模龐大，本位主義嚴重，不易彈性應變。倘若軍工央企組織結構無法大幅改革，或因容忍研發錯誤而導致高層「貪污腐敗」被整肅，對於民間企業的研發創新將造成嚴重阻礙。

二、解放軍AI軍事應用恐難超越美軍

事實上，解放軍的「智能化戰爭」處處模仿美軍，而中國民間

[4]〈從軍博會看解放軍如何使用 AI〉，《新浪財經》，2025 年 05 月 21 日，https://finance.sina.com.cn/jjxw/2025-05-21/doc-inexhsqh0547873.shtml?froms=ggmp。

[5]〈任皓：解放軍總醫院 DeepSeek 部署實踐經驗分享〉，《中國醫院協會信息專業委員會》，2025 年 3 月 3 日，https://www.chima.org.cn/Html/News/Articles/17254.html。

AI 企業也以美國 Palantir、Google 等公司為標竿。換言之，中共目前 AI 軍事應用仍落後於美國（表 2）。此外，解放軍自 1979 年中越戰爭之後毫無實戰經驗，民間企業只能依賴歷史資料或公開數據來訓練其軍事大模型，可能影響訓練及推理品質。另一方面，儘管中國在中低階機器人實體製造方面具有優勢，甚至開發出數款微型無人機，但是在機器人的「AI 大腦」，特別是 AI 運算能力上，受美國 AI 晶片管制而有所延滯。這是否影響解放軍未來無人武器平台或機器人軍隊的發展，尚待後續觀察。雖然中共亟欲在軍用 AI 領域超越美國，但長期而言恐仍難擺脫「模仿者」或「跟隨者」之角色。

表 1、中共軍工集團旗下 AI 研發創新機構

	軍工集團	名稱	成立時間及地點	研發重點
1	兵器工業	中兵智能創新研究院有限公司	2022.01，北京市	探月工程月球車（參研）、四足仿生機器人、機器人技術、群體協同與自主技術、無人系統、智能科技、啟元實驗室
2	兵器裝備	杭州智元研究院有限公司	2022.01，杭州市	軍事智能前沿技術、總體設計、感知增強、智能無人平台、智元實驗室
3	航天科工	航天科工集團智能科技研究院有限公司	2022.05，北京市	智能科技創新、智能體系研究、數位孿生技術與應用、航天智能、航天防務
4	航天科技	中國航天科技集團有限公司創新研究院	2022.07，北京市	智能系統與應用集成、先進探測與未來信息、智能算法與共性技術、智能測試與基礎平台、先進材料與新型能源、前沿交叉技術
5	中國電科	中國電科智能科技研究院	2021.12，北京市	央企集團首家先進科技創新平台。智能體系、智能基礎平台、感知認知、無人體系、雲數智一體化
6	中國船舶	中船智海創新研究院有限公司	2022.04，北京市	海上智能科技
7	航空	航空工業智航	2021，北	航空工業人工智能科技發展

	工業	院	京市	

資料來源：作者整理自各集團官網及公開資料。

表 2、美中兩國軍事 AI 應用及創新之初步比較

項目	美國	中國
AI 軍事應用實例	● 聚焦於情報收集分析、戰爭模擬、戰略規劃、決策支持、聯合作戰、自主武器、無人載具蜂群作戰、健康數據等。 ● 全自主無人作戰平台（Sheild AI、GA-ASI、Anduril） ● 協助決策（Palantir、Scale AI、Applied Intuition） ● 即時情報及態勢感知（MAG Aerospace）	● 聚焦於智能化作戰能力和系統整合，如：「戰顱」系統、「千手觀音」指控通訊系統（對標美國 JTACS 系統）、語音識別、圖像分析、自主武器、戰場通訊、機器狼／機器狗等。 ● 建立全球首個軍用 5G 系統，可同時連接 1 萬個以上的軍用機器人，進行大規模機器人協同作戰。 ● 利用開源大模型開發軍用 AI「ChatBIT」、DeepSeek 導入解放軍醫院。
AI 創新條件	多元民主社會、世界級 AI 研發人才、創投及私募基金充沛、新創企業眾多	國家主導之專制社會、政策規劃明確、政府資金大舉投入（超過 200 億美元）、各種資源容易集中
政府推動與民間企業合作	DoD 設有 DIU、AFWERX、聯合 AI 中心（JAIC）、首席數位及 AI 辦公室（CDAO）、陸軍設「201 部隊」授予 Meta、OpenAI、Palantir 主管中校軍階	採行「軍民融合」政策、軍工央企參與早期投資或參股、併購民間 AI 新創公司。另，解放軍向民間採購無人智能化裝備（機器狗、無人車）或醫院門診大模型服務平台
參與軍用 AI 之企業	微軟、谷歌、臉書（Meta）、亞馬遜、甲骨文（Oracle）、Open AI、Palantir、Anduril、Snowflake、Anthropic、×AI、Scale AI、Shield AI、GA-ASI、Applied Intuition、MAG Aerospace 等。	百度、商湯科技、科大訊飛、北京華天海峰、淵亭科技、宇樹科技、中科海訊、達闥科技等。

資料來源：作者整理自公開資料。

中共運用數位混合威脅升高灰帶衝突

曾怡碩

網路安全與決策推演研究所

焦點類別：灰色行動、網路戰、認知戰、中共網軍

壹、前言

世人熟知的網路數位空間攻擊，不論是近兩年來美國政府公布的中共對美國關鍵基礎設施與政府機關的「伏特颱風」、「亞麻颱風」、「鹽颱風」網路攻擊，[1]還是台灣政府機關每天遭受主要來自中共及其贊助駭侵團體高達 240 萬次的網路攻擊，[2]皆屬於網路數位衝突競爭的一部分。僅從削弱經濟運作的角度來看，網路空間可發動的攻擊手段已相當多樣化，除了透過滲透行動竊取營業秘密，或以大規模阻斷服務（DDoS）與延遲傳輸速度來降低資料可及性之外，攻擊行動也可能延伸至網路空間以外。例如，針對通訊衛星的太空攻擊或鎖定海底光纖網路的實體破壞，都可能被用來中斷關鍵網路服務，造成更深遠的衝擊。換句話說，網路數位衝突競爭包括實體空間與網路空間的攻防，橫跨領域包括太空、海底、網電，而影響衝擊領域還擴及到心理認知、經濟金融、民生醫療等，使用手段則含括網路攻擊手法、實體破壞進擊手段以及各式混合複合威脅。[3]

中共近來效法美國及其五眼聯盟夥伴揭露並起訴國安部外圍駭侵團體成員作法，接連揭露我國資通電軍網路聯隊成員，意圖製造情報滲透成功的威懾效應。鑒於中共對我國之網路衝突手法趨於多元複雜，實有必要盤點中共對臺網路衝突的混合威脅樣態，並檢視

[1] 〈美國制裁中國資安公司涉及「鹽颱風」駭客集團入侵事件〉，《資安人》，2025 年 1 月 23 日，https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=11585。

[2] 游凱翔，〈國安局：2024 年每日遭中共網攻 240 萬次 比前 1 年翻倍〉，《中央社》，2025 年 1 月 5 日，https://www.cna.com.tw/news/aipl/202501050041.aspx。

[3] Julia Voo and Virpratap Vikram Singh, “Competition in Cyberspace: A Distorted Representation,” *IISS Report*, April 24, 2025, https://reurl.cc/7VrKa9.

是否有藉此升高灰色地帶衝突，俾利我國預警與提前因應。

貳、安全意涵

一、網路威脅的灰色地帶衝突升級特徵

網路衝突與競爭，即使在多數情況下屬於低於戰爭門檻的「灰色地帶衝突」，但端視敵方所選擇的攻擊手段、目標與造成影響衝擊，可能造成衝突程度的升級，從競爭衝突衍生為危機、甚至遽升為武裝衝突或者戰略襲擊的層次。承平時期的網路空間競爭或惡意作為多被視為灰色地帶衝突，諸如運用網路滲透進行間諜竊密行徑、施行大規模阻斷服務攻擊對方政府機關，運用網路遂行認知作戰以對目標國之社會大眾進行干預操控（例如「駭入再散布」），這時候網路衝突其實已然跨越網路空間，意圖達成情報戰或心理戰的效應，只是仍以網路空間為資訊傳遞的主要載體。

當網路衝突進展到破壞政府機關運營與能源供應時，需檢視惡意敵方是否混搭運用傳統武力途徑或載台製造禍端——例如，在軍機艦騷擾之餘並伴隨電子情報蒐集、或者協同散布入侵領空領海合成照以遂行認知作戰。但更重要的是，要評估該類衝突造成衝擊是否為暫時性，還是要一段時間方能恢復，據以判定敵方是否藉網路數位混合威脅手段，意圖將灰色地帶衝突升高形成瀕戰危機，進而恫嚇脅迫受害國改變其政治現實。

具體而言，台灣曾經歷過的混合威脅，像是敵方以網路行動干預選舉、或干擾政府機關運作，甚至以勒索軟體病毒暫時癱瘓基礎設施或者能源供應輸送，仍屬灰色地帶衝突中較具威脅性的敵意舉動。倘若敵意網路衝突針對政府運作與能源接收、供應與傳輸進行非暫時性的破壞甚至阻斷，或者對於部隊移動、後勤補給進行阻斷，甚至阻斷指揮管制鏈通訊、持久性阻斷關鍵基礎設施運營——

例如切斷海底電纜，[4]均可視為敵方為接續戰爭爆發之戰場環境預作演練與準備，[5]實質上形同將狀況升高到瀕臨戰爭前的狀態。

易言之，該類作為雖仍屬灰色地帶衝突，但實質上是為接續戰場環境預作演練準備，因此該類作為可被視為灰色地帶衝突層級的升高。此外，鑒於國家行為者在從事灰色地帶衝突時，尤其是數位網路相關之行徑，往往委由包括網路傭兵在內的非國家身分代理人，因此在探討灰色地帶衝突升級之際，國家以及國家委外之代理團體所從事行為，均列入檢視範疇。[6]

二、數位混合威脅體現中共對台網路威脅樣態

中共對台施行網路威脅的樣態，最早是發動網路攻擊，讓台灣很早就躍升全球網路攻擊熱點，台灣民眾也從政府機關或所處企業或自身遭遇，深切體會資安防禦的重要性。國家安全會議於 2018 年 9 月公布台灣首部《國家資通安全報告》，確立「資安即國安」指導原則，將網路安全提升為國家安全高度並予以因應。另一方面，中共見證俄羅斯於 2016 年前後有效運用假訊息與認知影響力作戰干預美國及歐洲多國的選舉與國內政治，迅速予以仿效並以台灣為試驗場發起大規模認知作戰，搭配當時日益頻繁的對台軍機繞台及軍艦侵擾，放送空拍台灣景致的合成影像，[7]這算是中共數位混合威脅的初試啼聲。

中共在網路衝突的灰色地帶衝突並不僅侷限在網路空間領域的網路攻擊與認知作戰，還搭配或者延伸到情報作戰。中共不只一次

---

[4] Julia Voo and Virpratap Vikram Singh, “Competition in Cyberspace: A Distorted Representation,” *IISS Report*, April 24, 2025, https://reurl.cc/7VrKa9.

[5] James Van de Velde, “Cyber Deterrence Is Dead! Long Live ‘Integrated Deterrence’!” *Joint Force Quarterly* 109, 2nd Quarter, April 2023, https://reurl.cc/6qypmd.

[6] Jonathan Wilkenfeld and Devin Ellis, Escalation Management in the Gray Zone Shaping Decision Calculus: From Theory to Causal Understanding (Award No. N00014-18-1-2369) (College Park, US: University of Maryland, College Park, 2021), pp. 123-127.

[7] 呂欣憓，〈傳共機拍下玉山 國防部：勿以訛傳訛〉，《中央社》，2016 年 12 月 17 日，https://www.cna.com.tw/news/firstnews/201612175010.aspx。

運用假造公文捏造台灣情報單位的訊息，或者運用境外情工獲取之情資公告台灣情報首腦訪外行程，[8]形同其情報部門運用網路認知作戰對台情報單位公開叫陣。此外，2023 年台灣連結馬祖的兩條海底電纜遭切斷，導致一萬多馬祖居民沒有網路可用，雖然海纜遭破壞原因包括漁船拖網、船錨、及中國抽砂船等，[9]但馬祖周邊多為中國籍船隻，因此曾遭起疑這些事故恐為中共鑑於俄烏戰爭教訓了解切斷對外通訊的重要性，故運用灰色地帶代理船隻，藉台馬海纜演練日後如何切斷台灣對外通訊。[10]然而，由於台馬海纜並非連結台灣的國際海纜，加上台馬之間纜線 2018 至 2023 年 2 月在 5 年間遭斷超過 20 次，因此即便 2023 年兩條海纜同時中斷，仍難以明確判定為中共蓄意破壞的行為。[11]畢竟，原先只有一條海纜，但台灣在 2022 年俄烏戰爭爆發後記取教訓加速建立數位韌性，才鋪設新的海纜，如此才會發生兩條海纜遭切斷，而從前根本不可能發生這樣啟人疑竇的巧合。[12]

三、中共藉由對台數位混合威脅測試拉高衝突後各國反應

鑒於全球民主陣營持續關切台海和平穩定，加上美國川普總統國安團隊聲稱將專注因應中共，因此中共在 2025 年上半年對台進一步運用先前數位混合威脅經驗，意圖藉升高灰色地帶衝突情勢以測試關切台海情勢之民主國家反應。首先，繼 2024 年 9 月中共國安部公布台灣資通電軍網路戰聯隊 3 成員照片與個資後，於 2025 年 3 月

---

[8] 筆鋒，〈台官外訪曝光　兩岸情戰心戰〉，《亞洲週刊》2022 年第 40 期，2022 年 10 月 3 日，https://emag.yzzk.com/article/details/筆鋒/2022-40/1664421911806/台官外訪曝光%E3%80%80 兩岸情戰心戰。

[9] 〈馬祖電纜遭切斷暴露弱點 專家憂戰時聯外通訊不保〉，《中央社》，2023 年 3 月 15 日，https://www.cna.com.tw/news/aipl/202303150238.aspx。

[10] Elisabeth Braw, “China Is Practicing How to Sever Taiwan’s Internet: The Cutoff of the Matsu Islands May Be a Dry Run for Further Aggression,” *Foreign Policy*, February 21, 2023, https://foreignpolicy.com/2023/02/21/matsu-islands-internet-cables-china-taiwan/.

[11] 江明晏、蘇思云，〈台馬海纜中斷，中華電：近 5 年故障逾 20 次，暫不確信是否遭蓄意破壞〉，《中央社》，2023 年 2 月 16 日，https://www.cna.com.tw/news/aipl/202302160241.aspx。

[12] 楊智強，〈澎湖漁場、馬祖海纜全遭殃，中國盜砂船入侵的海峽風暴〉，《報導者》，2023 年 4 月 27 日，https://www.twreporter.org/a/china-dredging-penghu-matsu-destruction。

再度出手公布 4 員個資照片，接續由中共公安部進一步在 6 月由廣州市公安局擴大揭露 20 名網路戰聯隊成員之身分資料。[13]這一連串的動作在手法上其實並無新意，不過是刻意仿效美國及其友盟近年來多次追溯中共駭侵團體，經查證後公布身分並起訴中共解放軍及國安部駭客的作法。由於查證過程並非僅止於追查網路 IP，在實體上必須透過情報手法驗證個別成員身分與行為，因此中共此舉無疑是一邊向美國叫板表示將美國用在中共身上招數套用在台灣身上，同時再度向台灣情報單位叫陣炫耀在台的滲透情蒐能力。中共此番更進一步將資通電軍的網戰成員列入台獨制裁名單，不僅擴大了名單的公布規模，也刻意將網路衝突與情報戰、法律戰相互交織，模糊界線、強化其認知戰效果。此舉明顯延續美中網路與情報衝突路線，意圖挑釁刺激美台網戰與情報部門，除了拉高灰色地帶衝突情勢，同時觀察美國及其友盟的反應。

另一個值得關注的發展，則是延續 2023 年台馬海纜故障事件以及 2024 年底俄羅斯在波羅的海運用中國籍貨輪以船錨切斷通訊海底電纜與輸電纜的行動。2025 年 1 月初，喀麥隆籍貨輪的中國籍船長下令讓該輪在野柳外之海底電纜淺海鋪設處海床拖錨往返，[14]之後多次發現類似貨輪遂行同樣可疑舉動。有鑑於俄羅斯運用中國籍貨輪在歐洲破壞海纜的灰色地帶行徑足以造成能源與通訊基礎設施的非暫時性中斷，若搭配中共 2024 年「聯合利劍」系列以來之對台軍演被視為演練彩排對台動武，[15]中共運用「影子艦隊」切斷台灣周遭國

[13] 張淑伶，〈中國再稱遭國軍駭客攻擊 鎖定4名台軍現役人員〉，《中央社》，2025年3月17日，https://www.cna.com.tw/news/acn/202503170014.aspx；〈廣州公安局懸賞通緝 20 名台灣資通電軍人員〉，《中央社》，2025年6 月5日，https://www.cna.com.tw/news/acn/202506050036.aspx；廖士鋒、林則宏，〈觀察站／我資通電軍遭曝光 一次比一次詳盡〉，《聯合報》，2025年6 月5日，https://udn.com/news/story/10930/8788351。

[14] 劉建邦，〈野柳東北方海域海底電纜損壞 喀麥隆籍貨輪疑肇事海巡帶回調查〉，《中央社》，2025年1月4日，https://www.cna.com.tw/news/asoc/202501040120.aspx。

[15] 〈中國軍演：美軍說看到了解放軍的運作但警告或是攻台彩排〉，《法廣》，2024年5月26日，https://reurl.cc/yAn52M。

際海纜，顯然在表面上擺明是要測試民主陣營國家反應，其次則在於利用台灣民主體制下政府須對挑釁行為做出因應的特性，迫使我方增加海巡與海軍對海纜的巡邏與防護，藉此逐步消耗台灣的海上戰力與執法能量，俾利中共對台之不對稱作戰與長期消耗戰都能夠奏效。依照現在國際修復海纜的有限能量，未來倘若台灣十四條國際海纜均遭刻意切斷，阻斷台灣對外通聯將不只是暫時性，更可能造成經濟金融與社會人心動盪。因此，中共此番操作明顯有意藉數位混合威脅，升高灰色地帶衝突，藉此測試區域國家反應。

參、趨勢研判

一、中共將藉預演局部封控下調控衝突層級以測試區域國家反應

鑑於近兩年中共對台軍事演習聚焦於台海封鎖或隔離的想定，中共很有可能為避免屆時招惹他國而引發他國介入台海危機，因此中共最佳選項應為以升高、調降灰帶衝突方式，避免第三國介入中共對台之襲擾及封控。在此預設下，吾人可以預見中共在未來仍將持續演練灰色地帶衝突，並加入局部封控情境與數位混合威脅手段，測試周遭國家反應。例如當中共運用「影子艦隊」切斷台灣周遭國際海纜後，還派海警艦艇對於海纜修復船隻進行惡意阻擾，一旦受影響的區域國家表達嚴正關切而遭中共置之不理，當區域國家透露有意甚至派遣執法船隻甚至海軍戰艦前來海纜遭切斷水域，中共立刻撤回海警艦艇以降低關切熱度，如此反覆操作將可延長灰色地帶封控手段的持續時程，既可消耗台灣的因應資源與民心士氣，又能延長避免他國介入的時間。

二、中共將持續公開我資通電軍身分以遂行情報戰與心理戰

由於美國及其友盟對中共駭客之嚇阻除公告與起訴之外，還訴諸凍結個人金融帳戶，意圖製造嚇阻能力，中共可能持續將美國作法複製套用在台灣網路戰聯隊身上。然而，中共的金融制裁效應畢

竟受限於其管轄權與金融影響力，遠不能與美國相提並論，因此除了藉由經濟金融手段的制裁，亦可能藉公布相關人員之在中國大陸經商親友，試圖製造恐懼陰影並對相關人員形成更大的壓力。因此，未來可望見證中共持續公開我資通電軍網路戰聯隊成員身分，除藉由宣揚其情報戰之奏效，達到彰顯台灣軍隊無力防範中共滲透之心理威懾作用，還可能借助法律戰與經濟金融脅迫，達到孤立與施壓的心理戰綜效。

「資訊不在場證明」：當代戰爭中的資訊操弄

劉姝廷

國防戰略與資源研究所

焦點類別：認知戰、作戰概念

壹、前言

當代戰爭中的資訊操弄涵蓋多種策略操作，「資訊不在場證明」（information alibis）被視為一種新穎且獨特的策略。近期報告揭露「資訊不在場證明」被應用於俄羅斯對敘利亞的軍事介入以及俄烏戰爭之中，作為俄羅斯推動資訊武器化及其軍事戰略的一環，影響當代戰爭和國際輿論環境。[1]

烏克蘭國家安全與國防委員會「反虛假資訊中心」（Center for Countering Disinformation, CCD）對「資訊不在場證明」的定義，為「一方預先指控另一方即將從事其將要從事的行為，目的是為了推卸自身的犯罪責任」。[2]舉例來說，當俄羅斯想轟炸某處，其將提前指控烏克蘭將從事此行為，以掩蓋俄羅斯轟炸的真相和推卸戰爭罪責。[3]

本文依據前述報告內容，整理「資訊不在場證明」的操作邏輯：第一階段是「預防性指控」，預先指控對手實施其本要實施的行為；第二階段為「混淆受眾」，以假訊息使受眾認知陷入混亂而誤判；第三階段是「推卸責任」，掩蓋真相並主張不在場證明（如表1）。本文以此為基礎，分析俄羅斯以「資訊不在場證明」應用於當

[1] "Manufacturing Impunity: Russian Information Operations in Ukraine," *Global Rights Compliance*, May 8, 2025, p.3, https://reurl.cc/Rk6Ven.

[2] "The Use of Information Alibis by Russian Resources," *Centre for Countering Disinformation*, July 23, 2024, https://reurl.cc/nYVexe.

[3] "Ukrainian Resistance to Russian Disinformation," *RAND*, September 3, 2024, https://reurl.cc/yAnDyE.

代戰爭的案例，並嘗試從俄羅斯的案例延伸觀察中共可能仿效的趨勢，探討中共應用的情境、實現的條件及操作的模式，思考民主國家的因應之道。

表 1、「資訊不在場證明」的操作邏輯

階段	邏輯	解釋
1	預防性指控	預先指控對手實施其要實施的行為
2	混淆受眾	透過假訊息使受眾認知陷入混亂而誤判
3	推卸責任	掩蓋真相並主張不在場證明

資料來源：作者整理自“Manufacturing Impunity: Russian Information Operations in Ukraine,” Global Rights Compliance, May 8, 2025, p. 3, https://reurl.cc/Rk6Ven。

貳、安全意涵

一、訴諸輿論擴大策略效果

俄羅斯操作「資訊不在場證明」策略的特徵之一，是以平民與民用基礎設施為攻擊目標，透過資訊的虛構與扭曲等手法，將迫害平民的責任歸咎於對手，以此操縱民意和社會輿論。以 2015 年以來俄羅斯介入敘利亞內戰衝突為例，俄羅斯的立場是支持敘利亞政府對抗反對派。為此，俄羅斯除提供敘利亞政府武器，也採取軍事行動襲擊反對派控制區內的民用基礎設施，包括發電廠、變電站、醫院和教育機構等。鑑於此舉有違國際規範，俄羅斯乃先發制人。將攻擊平民的罪魁禍首指向反對派，藉由抹黑對手影響人民看法，掩蓋其與敘利亞政府襲擊民用基礎設施、傷害無辜民眾生命的真相。

實證資料顯示，自從俄羅斯介入敘利亞內戰衝突，敘利亞政府被發現更加系統化且廣泛的使用化學武器，[4] 2018 年 4 月 7 日，敘利亞度瑪鎮（Douma）遭到化學武器攻擊，造成大量平民傷亡。直到 2023 年 2 月 7 日，「禁止化學武器組織」（Organization for the Prohibition of Chemical Weapons, OPCW）的報告才證實敘利亞政府為

[4] “Death by Chemicals: the Syrian Government’s Widespread and Systematic Use of Chemical Weapons,” *Human Rights Watch*, May 1, 2017, https://reurl.cc/ekxlax.

此次攻擊的幕後黑手。[5]

事後來看，在 2018 年的事件中，俄羅斯政府先是指控「反對派正在準備使用化學武器針對敘利亞人民發動攻擊」；在攻擊發生之後，流傳「反對派將誣告敘利亞政府實施化學武器攻擊」等假訊息，誤導民眾將此次攻擊歸因於反對派行為。[6]在此之際，俄羅斯透過官方聲明與媒體宣傳，聲稱「沒有證據顯示度瑪鎮遭受化學武器攻擊」並捍衛敘利亞政府，[7]進一步將責任推向西方國家，指責西方國家以化學武器襲擊事件作為干預敘利亞的藉口。[8]

二、標籤化對手強化正當性

前揭俄羅斯介入敘利亞內戰衝突的案例顯示，搶先將對手貼上違法標籤是「資訊不在場證明」策略的重點，以凸顯自身行為的正當性，創造不利對手的作戰環境。這也反映在 2022 年以降的俄烏戰爭。俄羅斯將烏克蘭軍隊和政府官員塑造成製造戰爭的「罪犯」，先聲奪人指控烏克蘭「挑釁」引發爭端，散播大量未獲證實、內容涉及烏軍殘暴對待平民的影片，影響受眾對俄烏戰爭的看法，以此規避戰爭罪責。

俄烏戰爭爆發以來，烏克蘭民用建築、民用基礎設施及戰俘營接連遭受俄羅斯攻擊。在這些襲擊行動中，俄羅斯被發現利用各種媒體管道，如官方媒體、通訊軟體 Telegram 及軍事部落客操作「資訊不在場證明」策略。例如 2022 年 7 月 29 日，在烏克蘭境內、由俄羅斯控制的奧列尼夫卡（Olenivka）戰俘營遭襲擊爆炸，釀成大量

[5] "'Reasonable Grounds' to Believe Syrian Government Was Behind Deadly Chlorine Gas Attack on Douma: OPCW Report," *United Nations News*, February 7, 2023, https://reurl.cc/lYVxWl.

[6] "Manufacturing Impunity: Russian Information Operations in Ukraine," *Global Rights Compliance*, May 8, 2025, pp. 29-32, https://reurl.cc/Rk6Ven.

[7] "Syria Conflict: Russia Says No Evidence of Douma Chemical Attack," *BBC*, April 10, 2018, https://reurl.cc/9nEKZ8.

[8] 〈俄羅斯外交部長謝爾蓋•拉夫羅夫接受 BBC 新聞頻道"熱點話題"節目獨家採訪時的講話 莫斯科，2018 年 4 月 16 日〉，《俄羅斯聯邦外交部》，2018 年 4 月 16 日，https://mid.ru/cn/maps/gb/1568826/。

烏克蘭戰俘死亡。2023 年 7 月 5 日，聯合國人權辦公室（UN Human Rights Office）表示，儘管此起襲擊事件尚在調查階段，但經過大規模的訪談和分析，已證實爆炸並非由俄羅斯所指責的海馬斯（HIMARS）多管火箭系統引起。[9]此一階段性調查結果印證俄羅斯的資訊操弄。

進一步來看，俄羅斯操作「資訊不在場證明」的策略，並非在奧列尼夫卡戰俘營遭襲擊之後才開始，而是在襲擊行動前已見端倪。俄羅斯先在 Telegram 上大量傳播烏克蘭戰俘「承認」犯下戰爭罪的影片，藉此預先指控「烏克蘭軍隊與政府犯下戰爭罪」。在此鋪陳下，襲擊發生之後，Telegram 上出現一系列來自俄羅斯記者及軍事部落客提供的影片，包括「澤倫斯基下令處決自己的人民」、「奧列尼夫卡監獄現場發現烏克蘭『海馬斯』火箭殘骸」、「烏克蘭發動襲擊是為戰爭罪作證的戰俘噤聲」等未經證實的內容。[10]不久之後，俄羅斯駐聯合國代表與俄羅斯國防部發出聲明呼應前述說法，[11]將戰爭罪責歸咎於烏克蘭。

參、趨勢研判

一、中共將仿效應用於海上衝突

前述的個案顯示，衝突甚至戰爭行為的因果關係往往並非「不證自明」，而需要公正第三方花費時間與精力查證，這使俄羅斯可操作「資訊不在場證明」，混淆視聽並推卸責任。對台灣而言，須注意中共透過觀察和學習前述俄羅斯的案例，仿效這套以訴諸民意、標籤化對手為特色的策略，以「預防性指控」、「混淆受眾」及「推卸

[9] "UN Says Ukrainian POWs in Donetsk Not Killed by Rocket, as Russia Claimed," *Reuters*, July 25, 2023, https://reurl.cc/Rk1n0n.

[10] "New Report Exposes Russia's Strategic Disinformation Warfare," *Global Rights Compliance*, May 8, 2025, https://reurl.cc/Y3lz6n.

[11] 〈俄羅斯和烏克蘭相互指責對方對數十名烏克蘭戰俘被導彈炸死負責〉，《美國之音》，2025 年 7 月 30 日，https://reurl.cc/nY05ED。

責任」等邏輯手段進行在地化調整，應用於台海與印太區域。

事實上，中共可能已在南海領土主權爭端中逐步推進「資訊不在場證明」的策略。近年來中菲在南海屢有衝突，而中共反覆批判菲國違反國際法，對於己方的行動，則以含糊的「維權執法」帶過。2025 年 4 月 14 日，中菲雙方海警在南海爆發新一輪的衝突，中共即指控「菲方行徑嚴重違反國際法相關規定和海上避碰規則」等犯罪行為以此標籤化菲律賓海警，並以中共海警「依法巡邏」、「操作專業性規範」強調行為的正當性，稱此次衝突「責任完全在菲方」。[12]若將這些言論視為「預防性指控」，未來中共可能將製造衝突以落實菲方的挑釁或升高事態。例如，中共可能派遣海上民兵船駛入爭議海域並製造事端，藉此引發菲國海警的介入，中國海警再以保護本國漁民，以執法為由與菲方發生衝突，營造「混淆民眾」與「推卸責任」的資訊操弄基礎。

從上述案例延伸思考，掌握相關陰謀論與假訊息的傳播來源、路徑和影響層面相當重要，其可作為中共製造衝突前鋪陳「預防性指控」的預警訊號。對於民主國家的戰略溝通而言，預警的好處在於可增加己方的準備程度，也讓對手知道己方有所準備而降低真的採取行動之可能性。然而，預警機制對政府的戰略溝通也帶來限制，若反覆操作易造成「狼來了」現象，反而可能降低己方政府的可信度。因此，在中國海警近期頻繁侵擾我國海域的情況下，或可進一步根據衝突級別與影響程度，在戰略溝通上審慎使用預警策略。

二、中共將執法伺機製造衝突

將「資訊不在場證明」策略用於案例分析，可以理解中共資訊

[12] 〈菲海警船位黃岩島附近海域上演"碰瓷"鬧劇〉，《央視新聞》，2025 年 4 月 15 日，https://reurl.cc/A38qkK。

操弄的敘事邏輯，並藉由對照階段性操作邏輯觀察可能的線索，預測中共接下來的行為。除此之外，我們或許還可以進一步設想「資訊不在場證明」策略被中共操作的可能情境與實現之條件。

當前兩岸關係緊張的情勢下，中共持續透過擬定和擴大「台獨」頑固分子名單，發布《關於依法懲治「台獨」頑固分子分裂國家、煽動分裂國家犯罪的意見》，點名台灣政府官員、政治人物乃至政論節目主持人與來賓違背《反分裂國家法》等中國法律，[13]針對「台獨」關聯機構祭出制裁，[14]近期更聲稱「依法嚴懲」台灣八家實體公司等「台獨分裂勢力」，並實施出口管制。[15]

根據「資訊不在場證明」的操作邏輯，前述中共的行為尚處於標籤化對手的「預防性指控」階段。中共以法律與國家安全強化正當性，下一步或將依此敘事邏輯，挑選時機製造台灣民眾反對台獨的訴求，甚至歡迎中共接管台灣。如此一來，中共對台軍事行動將可以維護台灣秩序與穩定為名，既混淆台灣與國際視聽，更將責任推卸給台灣政府。近期有中共學者主張使台灣發生「第二次西安事變」，中共得以「保安」名義登島，訴諸輿論並強化正當性，從而實現統一目的。[16]這雖看似個人的激進言論，但也呼應「資訊不在場證明」的操作邏輯。

---

[13] 〈依法懲治「台獨」頑固份子〉，《中共中央臺灣工作辦公室》，https://reurl.cc/MzdZGm。

[14] 〈國台辦懲戒台灣民主基金會及國合會 禁與中國合作〉，《中央社》，2022 年 8 月 3 日，https://reurl.cc/3MLN9V。

[15] 〈漢翔等 8 家實體被陸列出口管制 國台辦表態支持〉，《經濟日報》，2025 年 7 月 9 日，https://reurl.cc/x30g8N。

[16] 〈陸學者稱二次西安事變統一台灣 台學者：應警惕武統手段〉，《中央社》，2025 年 7 月 13 日，https://reurl.cc/gY8Aq7。

歐洲因應俄國影子艦隊的實踐與啟示

李俊毅

國家安全研究所

焦點類別：國際情勢、灰色行動

壹、前言

2025 年 6 月 20 日，俄國護衛艦「敏捷號」（Boikiy）被發現以傳送偽造信號的方式隱蔽身分，於英吉利海峽西南端和兩艘受英國制裁的油輪會合，再北返俄國。論者認為，這是俄國首度以武力護航其影子艦隊（shadow fleet）的實例，顯示俄國面臨美歐國家制裁的壓力。[1]俄烏戰爭爆發以來，美國與歐洲為削弱俄國的軍事能力，對俄國施加經濟與能源制裁，導致後者仰賴以影子艦隊出口其石油。這些船隻多數經由波羅的海、北海乃至英吉利海峽往返，周邊國家打擊影子艦隊的實踐因此備受關注。2024 年 12 月 16 日，北歐波羅的海八國暨夥伴國家（Nordic-Baltic 8 ++, NB8++）發布聯合聲明，宣示採取協調的作法以干擾並嚇阻俄國的影子艦隊。2025 年 6 月 20 日，NB8++進一步以聯合聲明表示將在國際法的架構下提出一套政策指引，打擊俄國以影子艦隊規避國際制裁的行為。[2]在新的措施尚未明朗前，要求這些船隻出示相關保險證明，是當前歐洲國家打擊影子艦隊的主要實踐之一。7 月起，德國要求航經其海域的油輪需出示足以支付漏油危害的保險文件；瑞典則要求行經其領海或專屬經

[1] Ned Davies, Joshua Cheetham & Matt Murphy, “Russian Naval Ship ‘Disguised’ Itself While Passing Through English Channel,” *BBC News*, June 25, 2025, https://reurl.cc/7V26Al.

[2] 北歐波羅的海八國（Nordic-Baltic 8, NB8）為北歐五國（丹麥、芬蘭、冰島、挪威、瑞典）與波羅的海三國（愛沙尼亞、拉脫維亞、立陶宛）自 1990 年代起建立的非正式區域對話架構。NB8++則以 NB8 為基礎，納入第三方國家。前揭 2024 年 12 月的聯合聲明除這八國之外，另包含德國、荷蘭、波蘭與英國；2025 年 6 月的聯合聲明另加入比利時與法國。參見“Joint Statement on Further Action to Counter Russia’s ‘Shadow Fleet’,” *GOV.UK*, December 16, 2024, https://reurl.cc/bm55M3; “NB8++ Joint Statement on the Shadow Fleet,” *GOV.UK*, June 20, 2025, https://reurl.cc/Nxav06。

濟海域，以及停靠在該國港口的船隻出示相關保險證明。[3]

國際間對於影子艦隊的定義尚無共識。國際海事組織（International Maritime Organization, IMO）相對狹義的定義，稱其為「出於規避制裁、躲避安全或環境規範、逃避保險費用，或從事其他非法活動等目的，而從事非法行動的船隻」。此一定義以「非法」為影子艦隊的要項，實務上則多指為規避美國制裁而關閉追蹤系統，並掩飾其石油來源與目的地的船舶。[4]廣義的定義，則泛指利用老舊的權宜輪（flags of convenience）、國際海運錯綜複雜的所有權及管理結構，以及多種手段使使外界難以界定其行為的合法性之船舶。[5]一項報告稱截至 2024 年 5 月，全球運輸濕貨（wet cargo）——包括原油、石油產品與石化產品等——的船舶中，有 25%或 2,300 艘係屬廣義的影子艦隊。[6]

影子艦隊遊走於規範的灰色地帶，構成當前海洋治理的難題。歐洲國家為兼顧安全考量與基於航行自由之國際貿易，逐步嘗試制衡的方式應對。中國對台灣的海上灰色地帶威脅雖和俄國的影子艦隊不完全一樣，但歐洲的經驗或仍有可借鑒之處。

貳、安全意涵

一、影子艦隊的三重安全危害

影子艦隊的危害不僅止於走私遭制裁的石油，也對海洋環境、海事安全、與關鍵基礎設施等造成危害。首先是船舶本身的安全問

[3] "Germany, Sweden Enforce Insurance Checks from July 1 on Tankers to Combat 'Shadow Fleet'," *Shipping Telegraph*, July 3, 2025, https://reurl.cc/yAy2LO.

[4] "Resolution A.1192(33) Adopted on 6 December 2023 (Agenda Item 13) Urging Member States and All Relevant Stakeholders to Promote Actions to Prevent Illegal Operations in the Maritime Sector by the 'Dark Fleet' or 'Shadow Fleet'," *International Maritime Organization*, December 11, 2023, https://reurl.cc/K96NZR.

[5] Anna Caprile and Gabija Leclerc, "Russia's 'Shadow Fleet': Bringing the Threat to Light," *European Parliament Research Service*, PE 766.242, November 2024, https://reurl.cc/gYv9vz; "Shifty Shades of Grey: The Different Risk Profiles of the Dark Fleet Explained," *Lloyd's List Intelligence*, April 2023, https://reurl.cc/VW61OZ.

[6] "Updated: Illuminating Russia's Shadow Fleet," *Windward*, n.d., https://reurl.cc/2Q0D6n.

題。俄國遭受國際制裁後，需大量增加輸送石油的船隻，於是收購船齡超過 15 年的油輪。這些船隻不僅較易造成汙染，也因鮮少進行定期安全檢查且無誘因聘僱合格的海員，而容易發生意外。2023 年 5 月 1 日，油輪「Pablo 號」於馬來西亞外海起火爆炸，造成船上 3 名船員死亡，25 人獲救。該船於 1997 年建造，事發時的所有者不明，並曾數度更換船名、船旗與所有者，意外發生前 6 天方註冊於加彭，屬俄國影子艦隊之一。然而，因其所有者不明且無保險，馬來西亞政府需負擔滅火、搜救、打撈、清理與照護生存者等工作。[7] 同年 7 月 19 日，中資的超級油輪「Ceres I 號」與另一艘懸掛新加坡國旗的油輪「Hafnia Nile 號」於馬來西亞外海發生碰撞。分析指出，「Ceres I 號」多次運送遭美國禁運的伊朗石油至中國，而碰撞原因是該船發送虛假的位置訊號。[8]

其次是環境安全問題。前述兩個事例的「Pablo 號」與「Ceres I 號」皆於運送石油至中國後返航，未造成環境汙染。然而若這些船隻因事故造成大量漏油，將造成嚴重的污染。鑑於其所有權往往不明且未有可信賴的保險，相關費用勢將由沿岸國吸收，且求償無門。嚴重的污染除影響海洋生態系，也衝擊周邊國家的海洋經濟。

第三是對關鍵基礎設施的危害。2023 年 10 月 8 日，芬蘭和愛沙尼亞之間的天然氣管線「波羅的海連接管」（Balticconnector）遭懸掛香港旗幟、在中國註冊的船隻「新新北極熊號」（Newnew Polar Bear）以拖曳船錨的方式破壞。2024 年 11 月 17-18 日，兩條分別連接芬蘭與德國以及瑞典與立陶宛的海底光纖電纜疑似遭中國散裝貨輪「伊鵬 3 號」（*Yi Peng 3*）破壞，德國國防部長佩斯托瑞斯（Boris

[7] Elisabeth Braw, “The Threats Posed by the Global Shadow Fleet—and How to Stop It,” *Atlantic Council*, December 6, 2024, https://reurl.cc/1Ox1E8.

[8] Rebecca Tan, Pei-Lin Wu and Júlia Ledur, “‘Dark’ Tanker Crash Exposes Dangers of China’s Thirst for Cheap Oil,” *The Washington Post*, September 2, 2024, https://tinyurl.com/44ffztdx.

Pistorius）稱該事件為針對歐洲的「混合戰」（hybrid warfare）。[9]這兩起事件也引發沿岸國對此類船隻的法律權力之討論。

二、歐洲國家的制衡漸趨主動

歐洲國家打擊影子艦隊的作法大致有三：首先是制裁。歐盟自 2014 年起，即開始制裁受識別的俄國影子艦隊，並逐步擴大。調查顯示，在海事領域，2024 年 11 月受美歐等國制裁的船舶不到 1,100 艘，到 2025 年 5 月增加至約 1,600 艘，成長約 45%；同期受制裁的企業或實體則從 460 間增加至 670 間，成長 40%。其中，歐盟於 5 月 20 日提出第 17 輪的制裁，增加 189 艘受制裁的船舶，使總數達到 342 艘；英國則分別於 5 月 9 日與 20 日提出對俄制裁，共計制裁 110 艘影子艦隊船舶，以及若干實體與個人。這意味各國從被動地落實制裁規範，轉向積極甚至預防性地干擾與影子艦隊有關的網絡，透過情報與各司法機構的合作，將制裁的對象從油輪擴展到營運商、保險公司、管理人與中介商等支持影子艦隊運作的實體。[10]

其次是強化區域的監測與巡邏。2024 年 12 月 25 日，連結愛沙尼亞與芬蘭的「Estlink 2」海底電纜遭油輪「Eagle S 號」破壞。這導致區域國家在英國主導的「遠征軍聯合部隊」（Joint Expeditionary Force, JEF）架構下，於 2025 年 1 月展開「北歐看守」（Nordic Warden）任務，將英吉利海峽、北海、波羅的海等海域劃分 22 個區域，透過人工智慧分析自動識別系統（Automatic identification

[9] Finbarr Bermingham, “Beijing Admits Hong Kong-flagged Ship Destroyed Key Baltic Gas Pipeline ‘by Accident’,” *South China Morning Post*, August 12, 2024, https://reurl.cc/lYVngY; Sébastian Seibt, “Hybrid Warfare? China Sabotaging Baltic Sea Cables Would be ‘Super Surprising’, Experts Say,” *France 24*, November 21, 2024, https://reurl.cc/WOdz0x. “Has Denmark Challenged the Right of Innocent Passage? Watch Yi Peng 3 to Find Out,” *Lloyd’s List,* November 12, 2024, https://reurl.cc/EQ7Y6K.

[10] Dimitris Ampatzidis, “Navigating the Complexities of Maritime Sanctions: A May 2025 Overview,” *Maritime Traffic*, May 20, 2025, https://reurl.cc/x3ZRLN; “Russia’s War of Aggression Against Ukraine: EU Agrees 17th Package of Sanctions,” *Council of the EU*, May 20, 2025, https://reurl.cc/EQ7AMK; “UK Announces Major Sanctions in Support of Ukraine,” *UK.GOV*, May 20, 2025, https://reurl.cc/Ln3EQK.

system, AIS）與俄國影子艦隊的資料庫，進行即時監控與通報，以利各國回應。[11]

第三是要求船舶之保險證明。前述第一點的制裁，主要依據是船舶從事的行為（如是否運輸受制裁的石油）。歐洲國家進一步針對船舶本身的安全——亦即保險之有無——作為其是否為俄國影子艦隊的判準。國際航運的發達，使國際海事組織要求船舶所有人對其船舶須有適當的保險。然而海上事故一旦發生，其經濟代價十分高昂，非一般商業保險能保障。為降低營運風險，船東乃紛紛組成非營利性保險組織「船東互保協會」（Protection & Indemnity Club, P&I Club）。當前由全球 12 大「船東互保協會」組成的「國際集團船東互保協會」（International Groups of P&I Clubs）涵蓋全球 90%以上的國際商船總噸位。[12]俄國入侵烏克蘭後，「國際集團船東互保協會」因美歐對俄制裁，紛紛撤回對運輸俄國石油的船隻之保險。有無妥適的保險，乃成為識別俄國影子艦隊的依據。[13]

2024 年 10 月 17 日起，英國率先要求行經英吉利海峽的油輪出示保險證明，其理據是這些老舊船隻若缺乏適當的保險，將對海洋環境帶來高度風險。無保險或其保險是可疑的油輪，將受到制裁。此一實踐進一步落實於前述 NB8++的聲明以及若干區域國家的作法。被制裁的船隻，將無法使用歐盟與英國的港口、船閘，以及若干與海運有關之服務。[14]

---

[11]「遠征軍聯合部隊」由英國、冰島、丹麥、挪威、荷蘭、拉脫維亞、立陶宛、愛沙尼亞、瑞典和芬蘭等 10 國組成。參見“Joint Expeditionary Force Activates UK-led Reaction System to Track Threats to Undersea Infrastructure and Monitor Russian Shadow Fleet,” *UK.GOV*, January 6, 2025, https://reurl.cc/Ln395x。

[12] 蔡信華，〈船東互保協會法制之研究—以英國發展為核心〉，《興大法學》，第 24 期，2018 年 11 月，頁 205-261；Craig Kennedy, “Making the Baltic a ‘Shadow-Free’ Zone,” *Brookings*, July 2024, https://reurl.cc/1OxnqY.

[13] Elisabeth Braw, “The Threats Posed by the Global Shadow Fleet—and How to Stop It,” *Atlantic Council,* December 6, 2024, https://reurl.cc/VW6GgA.

[14] Michelle Wiese Bockmann, “UK to Check ‘Shadow Fleet’ Tankers for ‘Suspect, Dubious’ Insurance During English Channel Transits,” *Lloyd’s List*, October 17, 2024, https://reurl.cc/rYxzOO.

這些作法的成效仁智互見。論者認為，「國際集團船東互保協會」敦促其成員遵守美歐的制裁，因此即使是中國國企的油輪，亦將其船舶撤出與俄國的貿易。亦有報導指出，絕大多數受制裁的油輪，面臨遭閒置的命運，顯見制裁的成效。另一方面，相對於為數眾多的影子艦隊，遭制裁的船隻仍屬少數，且俄國亦不斷變更這些船隻的船名與船旗國，或購入其他船隻。[15]

參、趨勢研判

一、法律戰成為打擊影子艦隊的重心

影子艦隊之所以成為國際議題，係因其遊走於航行自由與海事安全的灰色地帶，構成相關國家決策的困難。《聯合國海洋法公約》（United Nations Convention on the Law of the Sea, UNCLOS）保障公海的航行自由，即使是在沿岸國的領海，外國船舶一般也享有無害通過權（innocent passage）。這造成打擊影子艦隊的困難。無論是船隻的狀態不良、缺乏有效保險，或運載受制裁的石油，都難以構成停止航行、登檢甚至扣留的理由。前述歐洲國家要求油輪出示保險的作法，並不影響船舶的航行，而僅是事後的制裁；這既以沿岸國有保護海洋環境的責任為由，又不干預航行自由，是兼顧自由與安全的作法。

儘管如此，歐洲國家仍持續探討更多的法律工具。就國際法的限縮而言，2024 年 11 月間，兩條波羅的海的海底電纜疑似遭破壞後，丹麥政府未證實「伊鵬 3 號」遭扣留，而僅確認該國海軍「緊靠」該船，引發無害通過權是否適用的爭議。2024 年 12 月，「Estlink 2」海底電纜遭破壞後，芬蘭海警要求有嫌疑的「Eagle S 號」油輪駛入芬蘭領海，從而登檢與扣留該船。由於遭破壞的海纜

[15] Craig Kennedy, “Making the Baltic a ‘Shadow-Free’ Zone,” p. 4; Eleanor Thornber and Julian Lee, “Dozens of Sanctioned Russian Oil Tankers Are Sitting Idle All Over the World,” *Bloomberg*, July 10, 2024, https://reurl.cc/yAg1Qq.

位於芬蘭領海之外，這亦引起沿岸國是否有權查扣相關船隻的爭議。[16]這兩個個案的法律爭議不僅攸關周邊國家查緝影子艦隊的依據，對其他地區與國家（如台海與南海）亦有深遠啟示。

就國際法的創設來說，報載 2025 年 2 月間，歐洲國家以閉門方式探討扣留俄國影子艦隊的法律依據。第一種可能性，是以危害當地海洋環境為名，扣押可能造成漏油事件的老舊油輪。其次，是將危及關鍵基礎設施的船隻界定為海盜。第三則是透過各國國內法，扣留未有妥適保險的船隻。[17]究實而言，三個方案都有法律上的挑戰，但歐洲若可提出符合海洋法的主張，亦將影響其他地區的實踐。

二、打擊影子艦隊越趨倚賴科技的應用

在當前的國際法環境下，停止、登臨與扣留可疑的船舶須有相當堅實的理由。丹麥即抱持高度審慎的態度，認為僅在船舶非無害通過的情況下，該國方有干預的正當性。然而，這往往需要對特定船舶有一定的了解，例如船員的安全與工作環境、保險，以及是否汙染當地海洋環境等。[18]覺察海域與船隻狀況的能力，因此攸關國家海洋治理的有效性。衛星偵照提供高解析度的圖像，有助於識別船隻的動態與可疑的活動，可增進國家快速反應的能力與介入的正當性。此外，英國領銜的「北歐看守」行動，應用人工智慧分析大量的船舶自動識別系統資訊與影子艦隊的資料庫，從而可以建立船舶的行為模式與風險程度，並預測其可能的欺瞞行為，亦是對抗影子艦隊的利器。

對台灣與印太地區國家而言，分享彼此對可疑或高風險的船隻

---

[16] "Has Denmark Challenged the Right of Innocent Passage? Watch Yi Peng 3 to Find Out," *Lloyd's List,* November 22, 2024, https://reurl.cc/3MLrdM; "Eagle S Owners Could Abandon Tanker, Lawyer Says," *Lloyd's List*, January 15, 2025, https://reurl.cc/gYmkLQ.

[17] Victor Jack and Gabriel Gavin, "Inside the New Plan to Seize Russia's Shadow Fleet," *Politico*, February 10, 2025, https://reurl.cc/89nlly.

[18] "Has Denmark Challenged the Right of Innocent Passage? Watch Yi Peng 3 to Find Out," *Lloyd's List*.

之資訊，應是強化區域海洋秩序與對抗中國海上灰色地帶威脅的第一步。在共同圖像的基礎上，區域國家方能進一步探討應用科技蒐集、分析與呈現可疑船舶的行為之架構或方式，藉此駁斥中國過度的主權聲張與脅迫，建立區域對海洋秩序的敘事。

英國海軍執行「高桅行動」的戰略意涵

江炘杓

國防戰略與資源研究所

焦點類別：國際戰略、印太區域

壹、新聞重點

2025 年 4 月 22 日，皇家海軍以威爾斯親王號航艦（HMS Prince of Wales, R09）為旗艦，編成「2025 航艦打擊支隊」（Carrier Strike Group, CSG25），支隊各艦分別自英國樸茨茅斯（Portsmouth）和普利茅斯海軍基地（Plymouth）啟航，執行為期八個月的印太部署，以「高桅行動」（Operation Highmast）為任務代號。部署期間陸續與澳洲、加拿大、法國、印度、義大利、日本、馬來西亞、紐西蘭、挪威、新加坡、南韓、西班牙及美國（依英文國名字母順序排列）等 13 國艦艇及其他觀察員於不同海域實施聯合演習，演習空間涵蓋海、陸、空和網路作戰。[1]

貳、安全意涵

2023 年 12 月 13 日，英國前國防部長夏普斯（Grant Shapps）宣布英國航艦打擊支隊將於 2025 年前進印太，並訪問日本等國。[2] 2024 年 10 月 26 日，施凱爾（Keir Starmer）首相為半年後（2025 年 4 月）的印太兵力展示明確表態：旨在「『向印太傾斜』（Indo-Pacific tilt），以抗衡中共正在增長的影響力」，並通過與太平洋島國聯合巡邏、打擊非法捕魚等行動，強化區域安全合作，增加在印太地區的軍事存在。[3]英國威爾斯親王號航艦自 2019 年 10 月服役以來，首次

[1] FORUM Staff, "U.K.-led Operation Highmast Departs for Indo-Pacific Deployment with Allies and Partners," *Indo-Pacific Defense Forum*, May 6, 2025, https://ipdefenseforum.com/2025/05/u-k-led-operation-highmast-departs-for-indo-pacific-deployment-with-allies-and-partners/.

[2] Ministry of Defence, "UK Carrier Strike Group to Visit Japan in 2025," *GOV.UK*, December 14, 2023, https://www.gov.uk/government/news/uk-carrier-strike-group-to-visit-japan-in-2025.

[3] David Lynch, "Royal Navy to Expand Patrols in Pacific Ocean, Starmer Announces," *Independent*,

航駛印太地區，CSG25 聯合兵力編組如表 1。

表 1、「高桅行動」航艦打擊支隊 2025 兵力編組表

國家	兵力
英國*	威爾斯親王號航空母艦（HMS Prince of Wales, R09）、無畏號驅逐艦（HMS Dauntless, D33）、李奇蒙號巡防艦（HMS Richmond, F239）、Astute級核動力攻擊潛艦和潮汐之泉號油船（RFA Tidespring, A136）
澳洲	雪梨號驅逐艦（HMAS Sydney, DDG42）
加拿大	魁北克號巡防艦（HMCS Ville De Quebec, FFH332)
紐西蘭	原力號巡防艦（HMNZS Te Kaha, F77）
挪威	阿蒙森號巡防艦（HNoMS Roald Amundsen, F311）、莫德號綜合補給艦（HNoMS Maud, A530）
西班牙	門德茲・牛內茲號巡防艦（ESPS Mendez Nunez, F104）
* 本次任務有4,500名英國軍人參與，包括600名空軍（含617中隊9架F-35B機組人員）、900名陸軍、2,500名海軍水手和陸戰隊以及艦載攻擊機（815中隊）、反潛直升機（814中隊）、運輸直升機（820中隊）和無人機（700X中隊）以及9架F-35B（809中隊）等500名機組人員。	

資料來源：Dzirhan Mahadzir, "The Royal Navy's Pacific Test," *USNI News*, June 27, 2025, https://news.usni.org/2025/06/27/the-royal-navys-pacific-test. 作者整理製表。

威爾斯親王號航艦打擊支隊執行「高桅行動」的主要安全意涵分析如下：

一、凸顯「印太」與「歐大」對英國同樣重要

英國「高桅行動」主要在地中海、阿拉伯海、印度洋、東南亞和太平洋實施雙邊或多邊軍事演習，並對希臘、新加坡、印尼、澳洲、日本、韓國、印度進行港口訪問。參照坎培拉大學歷史與海事戰略教授當雷（Richard Dunley）觀點：英國在印太地區最重要的安全夥伴是澳洲和日本，英國部署 CSG25 最明顯的效益就是展示其持續防衛能力及與區域夥伴的合作關係。[4]可見其長達八個月的海上部署，主要目的是強化英國與印太夥伴的安全聯繫關係，凸顯「印度洋－太平洋」與「歐洲－大西洋」對英國同樣重要，不可分割。

October 26, 2024, https://www.independent.co.uk/news/uk/pacific-ocean-royal-navy-keir-starmer-prime-minister-hms-prince-of-wales-b2635954.html.

[4] Alec Smith, "How Does the Deployment of Carrier Strike Group 2025 Benefit Britain?" *The Big Ask*, No. 17, April 25, 2025, https://www.britainsworld.org.uk/p/the-big-ask-17-2025.

二、通過聯合演習和港口訪問強化區域安全關係

英國 CSG25 是繼伊莉莎白女王號航艦（HMS Queen Elizabeth, R08）打擊支隊 2021 年部署印太海域以來第二次前進印太地區，透過與相關國家聯合軍事演習和港口訪問，加強與北約（North Atlantic Treaty Organization, NATO）和印太地區國家的安全聯繫關係。同時透過內部協同訓練，提高組合作業能力；並藉多國聯合演習提高聯盟作戰能力，操演項目包括：

（一）地中海打擊操演

威爾斯親王號航艦打擊支隊的兵力組成，除英國海軍驅逐艦、巡防艦、核動力攻擊潛艦和油船外，還有澳洲、加拿大、紐西蘭、挪威和西班牙軍艦加入CSG25編隊。支隊啟航後於4月28日抵達那不勒斯北約聯合司令部，5 月 5 日至 11 日在義大利塔蘭托和西西里之間的愛奧尼亞海，與義大利海軍加富爾號航艦打擊支隊（ITS Cavour, CVH550）實施「地中海打擊演習」（Exercise Med Strike）（北約年度「海王星打擊[Neptune Strike 25-1]演習」的一環）；另外還有加拿大、法國、挪威、葡萄牙、西班牙、土耳其和美國各類型艦艇，操演課目包括反潛作戰、水面作戰、制空作戰、兩棲作戰和無人機反制行動等，形同為 CSG25 前進印太舉行一場開幕式和熱身運動。

（二） 通過操演

6 月 9-10 日於北阿拉伯海與印度海軍塔巴爾號巡防艦（INS Tabar, F44）、潛艦和 P-8I 反潛巡邏機實施「通過操演」（Passage Exercise, PASSEX 25），操演課目包括反潛作戰、複雜戰術運動、整合式直升機管制作業以及海軍軍官專業交流，強化兩國對海上安全合作承諾與雙邊關係。[5]演習期間，英國空軍 617 中隊一架 F-35B 閃

[5] TOI News Desk, “PASSEX 2025: INS Tabar Joins UK Carrier Strike Group in Arabian Sea,” *The Times*

電 II 型戰機機件故障，緊急迫降於印度喀拉拉邦首府特里凡得琅國際機場，CSG25 航空工程師於三天後飛抵檢查，初步研判為液壓系統故障。

（三）護衛軍刀 2025

英國航艦支隊離開新加坡後，駛澳洲海域參加美國和澳洲主導的第 11 屆「護衛軍刀 2025」（Talisman Sabre 2025）多國聯合軍事演習，19 個國家共三萬多人參與，陸上演習區域第一次延伸至巴布亞新幾內亞。[6]英國航艦於本次演習將出動八架 F-35B 戰機參演。演習時間自 7 月 13 日起至 8 月 4 日止持續 24 天，期間並將與美國航艦支隊進行「雙航艦」操演，通過這次多國聯合演習展現其 F-35B 的「全面作戰能力」（Full Operational Capability, FOC）。

威爾斯親王號航艦打擊支隊於演習後將對澳洲達爾文進行港口訪問，而後駛日本橫須賀和韓國釜山，並將在日本舉辦「太平洋未來論壇」（Pacific Future Forum），聚焦於探討區域安全面臨的挑戰以及軍事科技發展，其後分別與日本和韓國海軍進行聯合操演。已知 CSG25 將與日本海上自衛隊（JMSDF）加賀號（JS Kaga, DDH-184）航艦編隊演練提高互操性（F-35B 互降對方航艦）、聯合防空與強化海域感知能力。

（四）「五國團結」聯合演習

英國航艦支隊預定於 2025 年 10-11 月間與澳洲、馬來西亞、紐西蘭和新加坡「五國防禦安排」（Five Power Defence Arrangements, FPDA）機制成員舉行海空聯合演習，並在印度洋海域與印度軍隊實施雙邊聯合操演，其後順訪印度孟買。

---

of India, June 11, 2025, https://timesofindia.indiatimes.com/india/passex-2025-ins-tabar-joins-uk-carrier-strike-group-in-arabian-sea-see-pics/articleshow/121778441.cms.

[6] 參加本屆「護衛軍刀2025」的國家除了主辦方美國和澳洲之外，還包括加拿大、斐濟、法國、德國、印度、印尼、日本、荷蘭、紐西蘭、挪威、巴布亞新幾內亞、菲律賓、韓國、新加坡、泰國、東加和英國；另汶萊、馬來西亞和越南派遣觀察員參加。

威爾斯親王號航艦打擊支隊部署印太大事記如表2：

表 2、威爾斯親王號航艦打擊支隊部署印太大事記

日期	事件
4月14日	皇家海軍潮汐之泉號油船完成支援CSG25遠洋部署戰備整備，向支隊旗艦報到應遣
4月17日	23型巡防艦李奇蒙號完成Link 16系統安裝測試，可透過衛星傳送戰術資料，具「視距外」情報整合與分享能力
4月20日	加拿大海軍魁北克號巡防艦抵達英國樸利茅斯海軍基地，向旗艦威爾斯親王號報到納編支隊
4月22日	各艦分別於樸茨茅斯和普利茅斯港啟航，執行「高桅行動」印太地區部署任務
4月23日	挪威海軍阿蒙森號巡防艦和莫德號補給艦於英倫海峽與編隊會合，加入航艦打擊支隊
4月25日	海、空軍F-35B戰鬥機、各型直升機和無人機中隊自陸上基地起飛，先後降落威爾斯親王號航空母艦
4月28日	西班牙海軍門德茲・牛內茲號巡防艦於直布羅陀西端與編隊會合，加入航艦打擊支隊
4月29日	進入地中海，準備參加聯合軍事演習
5月5日	與北約各國海軍實施「地中海打擊」聯合演習，為部署印太暖身
5月12日	與義大利加富爾號航艦打擊支隊會合實施雙邊聯合操演，置重點於F-35B聯合制空和聯合反潛
5月14日	駛抵希臘克里特島和蘇達灣泊港休整
6月3日	通過蘇彝士運河和紅海，進入印度洋
6月9日	與印度海軍展開兩天「通過操演」
6月14日	一架F-35B因液壓系統故障，迫降於印度喀拉拉邦首府國際機場
6月18日	紐西蘭海軍原力號巡防艦加入CSG25
6月23日	1. 抵新加坡濱海灣郵輪碼頭，展開進入印太地區第一站港口訪問 2. CSG25魁北克號巡防艦與馬來西亞海軍巡防艦來吉爾號（KD Lekiu）實施「通過操演」，隨後訪問馬國巴生港
6月25日	CSG25李奇蒙號和門德茲・牛內茲號巡防艦訪問印尼丹戎不碌港
6月29日	澳洲雪梨號驅逐艦加入CSG25
7月13日	參加「護衛軍刀2025」聯合軍事演習
8月4日	訪問澳洲達爾文港
8-9月	1. 訪問日本橫須賀和韓國釜山，分別與日、韓實施聯合軍事演習 2. 於橫須賀舉辦「太平洋未來」論壇
10月	與新加坡「五國防禦安排」（FPDA）實施「五國團結演習」，中停新加坡整補
11月	與印度海、空軍實施雙邊聯合演習，順訪印度孟買，F-35B修復飛返威爾斯親王號航艦
12月	經紅海、蘇彝士運河、地中海、大西洋返回英國

資料來源：作者蒐集網路公情綜合整理製表。

三、英國航艦打擊支隊前進印太的目的

「高桅行動」顯然不是單純投射硬實力。2024 年 9 月止，印太地區佔英國貿易總額的 17%，達 2,860 億英鎊。[7]英國為維護經貿利益，有充分理由於印太地區展現軍事存在，主要目的有四：一是保護重要海上航道，確保經貿利益安全。二是支持以規則為基礎的國際秩序，確保自由航行和合法的海上行為。三是展示可信的海上力量，支援盟友安全，並向潛在對手發送嚇阻信號。四是透過一系列聯合軍演與港口訪問展示英國海軍的硬實力和軟實力，並為其軍工企業產品爭取貿易機會。

四、通過聯合編組強化聯盟作戰能力

英國海軍威爾斯親王號航艦打擊編隊納入澳洲、加拿大、紐西蘭、挪威和西班牙艦艇，形成「北約－印太」海軍聯合編隊（外軍艦艇數量比英國海軍還多），一方面可以節約英國海軍兵力，另一方面外軍艦艇也有機會結伴參加遠海長航訓練；既是一種共同提升的雙贏安排，也是聯盟海軍遠洋兵力投射的一種新模式；通過聯合編組有利強化聯盟間的聯合作戰能力。同時也是落實英、法之間的鬆散協議：兩國航艦打擊支隊輪流前進印太，以保持歐洲在該地區軍事存在的一種實踐。[8]

參、趨勢研判

一、英國將在印太地區保持軍事存在

航艦打擊支隊長黑摩爾准將（Commodore James Blackmore）表示，「CSG 2025 關乎維護以規則為基礎的國際秩序，並確保自由開

[7] Yuvraj Tyagi, “Britain Launches 8-Month Carrier Strike Group Mission ‘Operation Highmast’ for Indo-Pacific with 4000 Troops,” *Republic World*, April 9, 2025, https://reurl.cc/ko0vZd.

[8] 法國戴高樂號航艦（FS Charles de Gaulle, R91）打擊支隊已於 2025 年上半年離開印太地區返回歐洲。見 Edward Black and Sidharth Kaushal, “Necessity of Evolution: CSG Deployment After Highmast,” *RUSI*, June 11, 2025, https://reurl.cc/z5zO5N.

放的印太地區與歐洲貿易利益」。[9]研判英國軍事力量會在印太地區保持長期存在，目前英國海軍添馬號（HMS Tamar, P233）和史佩號（HMS Spey, P234）巡邏艦已經持續在本地區進行長期巡邏，履行英國對本地區夥伴的安全承諾。隨著與地區合作關係加深，英國在印太地區部署航艦打擊支隊的可能性大增。

二、英國將在印太安全扮演重要角色

藉由「高桅行動」任務使英國成為可靠的印太安全夥伴。英國航空母艦在印度洋－太平洋部署不僅是一種海軍艦隊運動，也是英國對地區和平、自由貿易和盟國防衛承諾的象徵。「高桅行動」顯示英國皇家海軍已準備好與合作夥伴並肩，共同確保海洋安全。英國可能會透過 FPDA 以及 QUAD 機制強化其參與程度，未來威爾斯親王號和伊莉莎白女王號航空母艦輪流在印太海域部署，預示英國將在印太安全議題扮演更重要角色。

[9] Kelly Ng and Steve Lai, "UK Aircraft Carrier in Indo-Pacific on Rare Deployment," *BBC*, June 25, 2025, https://www.bbc.com/news/articles/cx2gp07yqnjo.

運用退火計算於反制空中威脅之模擬

賀增原

網路安全與決策推演研究所

焦點類別：不對稱作戰、國際情勢

壹、前言

6 月 13 日以色列摧毀伊朗核設施與軍事基地，同時殲滅多名高階軍官與專業科學家，伊朗即刻以飛彈與無人機報復攻擊以色列。這使得以色列引以為豪的多層次防空系統遭遇突穿，並且造成數百人輕重傷以及死亡。[1]據此，本文擬由模擬量子退火計算來說明反制空中來襲的威脅，包含飛彈與無人機，企圖找出最佳化防空武器部署方式。

退火計算（annealing）包括量子退火和數位退火兩類技術，量子退火主要是採用量子力學的穿隧特性找尋全域當中最佳解，企圖避開陷入局部最佳解。[2]數位退火分為模擬退火（simulated annealing, SA）和模擬量子退火（simulated quantum annealing, SQA）2 類。[3]而本文採用數位退火中二次無限制二進制最佳化（Quadratic Unconstrained Binary Optimization, QUBO）形式建模，同時運用生成式 AI（Microsoft Copilot）求出反制空中威脅的最佳解。本文參考此次戰役，整理資料後發現，伊朗分別用法塔（Fattah）、[4]柯蘭沙爾飛

---

[1] 李羿璇，〈美以襲擊核設施後局勢升溫　伊朗宣布暫停與國際原子能總署合作〉，《CTWANT》，2025 年 7 月 3 日， https://www.ctwant.com/article/428571/。〈以色列防空飛彈恐只能再撐 10 天、需美支援？以軍方不評論〉，《anue 鉅亨》， 2025 年 6 月 19 日，https://news.cnyes.com/news/id/6029744。

[2] 張慶瑞，〈量子科技革命〉，《現代財經基金會》， 2022 年 4 月，頁 238-252。

[3] 于廉波、陳志宇、張慶瑞，〈後摩爾定律時代的新興量子計算技術—退火計算〉，《台灣半導體產業協會簡訊》，第 97 期，2021 年 7 月，頁 2-7。

[4] 倪浩軒，〈伊朗發射「法塔」極音速飛彈！真能打穿以色列鐵穹？影響一次看〉，《今日新聞》，2025 年 6 月 18 日，https://www.nownews.com/news/6696947。周辰陽，〈伊朗宣稱「極音速飛彈」　突破以色列防空系統〉，《聯合新聞網》，2025 年 6 月 19 日，https://udn.com/news/story/124061/8816458。

彈-4（Khorramshahr-4）、[5]以及無人機轟炸以色列；而以色列則以包含薩德系統(THAAD)、箭式系統（Arrow System）、大衛投石索（David's Sling）與鐵穹（Iron Dome）等系統針對不同的空域來防禦。因此本文模型採用：建置一個區域具有 4 種不同防空飛彈系統，同時面臨來襲的 3 種空中威脅（包含飛彈與無人機）。限制條件至少有 3 項：一、一種防空武器至少要接一個威脅飛彈或無人機；二、面臨來襲的空中威脅飛彈或無人機至少有一種防空武器去接戰；三、如果對於來襲的空中威脅飛彈或無人機，發射一枚防空武器去接戰，如果攔截失敗，被空中威脅飛彈突穿，此時至少再發射一種防空武器去攔截。本文利用以下章節來說明求解過程與結果。

貳、安全意涵

一、數學建模評估反制效應

首先定義決策變數，有 4 種防空飛彈系統（A_1, A_2, A_3, A_4），其中 A_1 代表負責高空防禦飛彈系統的薩德系統；A_2 箭式系統主要攔截長程彈道飛彈；A_3 代表大衛投石索系統，負責中空層的防禦；A_4 以鐵穹系統代表，負責短程防空系統。3 種空中威脅飛彈或無人機（T_1, T_2, T_3），其中 T_1 代表法塔為極音速飛彈；T_2 以柯蘭沙爾飛彈-4 代表, T_3 則是以無人機為例（本文無人機用見證者 129（Shahed-129)），整理上述描述為表 1、2。

[5] 吳映璠，〈影》川普空襲後伊朗首轟！「最大飛彈」炸以 86 傷〉，《中時新聞網》，2025 年 6 月 22 日，https://www.chinatimes.com/realtimenews/20250622001910-260408?chdtv。

表 1、以色列防空系統

系統代號	系統名稱	攔截防禦	反制威脅
A_1	薩德	戰區高空	長程彈道飛彈
A_2	箭式	長程高空	長程彈道飛彈
A_3	大衛投石索	中空層	中程飛彈
A_4	鐵穹	短程低空	無人機、短程飛彈

資料來源：作者自行整理。

表 2、伊朗空中威脅

威脅代號	系統名稱	類型	特性
T_1	法塔	極音速飛彈	高速、長程、高空
T_2	柯蘭沙爾飛彈-4	中長程彈道飛彈	彈道軌跡、中高空
T_3	見證者 129	長航時無人機	低空、慢速、飽和攻擊可能性

資料來源：作者自行整理。

決策變數令 x_{ij} 表示防空飛彈系統 A_i 是否攔截空中威脅 T_j，其中在 QUBO 建模中以二元變數來識別，當攔截成功以 1 表示，當攔截失敗以 0 表示，亦就是 x_{ij}=1 代表防空飛彈系統 i 成功攔截空中威脅 j；x_{ij}=0 代表防空飛彈系統 i 攔截空中威脅 j 失敗。

接著將限制條件以數學式來表示：

1. 每種防空飛彈系統至少要攔截一個空中威脅

$$\sum_{j=1}^{n=3} x_{ij} \geq 1, \forall i \in \{1,2,3,4\} \quad (1)$$

2. 每種空中威脅至少要一個防空飛彈系統攔截

$$\sum_{i=1}^{m=4} x_{ij} \geq 1, \forall j \in \{1,2,3\} \quad (2)$$

3. 若攔截失敗，至少需要另一種防空飛彈系統進行第二次攔截

$$\sum_{i=1}^{m=4} x_{ij} + y_i \geq 1, \forall j \in \{1,2,3\} \quad (3)$$

其中 y_i 代表額外增加攔截的武器決策。

最後設計目標函數，本文的主要目標是建立使用最少的防空飛彈數量，數學式

$$min \sum_{i,j}^{n=3,m=4} c_{ij} x_{ij} \quad (4)$$

其中 c_{ij} 代表每種防空飛彈的資源成本。

在此設定的條件使用生成式 AI（Microsoft Copilot）將 QUBO 轉換為矩陣形式（適用於 D-Wave 或其他量子/近似解法）去求解，可以獲得以下的結果（如表 3）。

表 3、模擬退火器得到的最佳解

防空系統/威脅	法塔	柯蘭沙爾飛彈-4	見證者 129
薩德	✅	❌	❌
箭式	❌	✅	❌
大衛投石索	❌	✅	✅
鐵穹	✅	❌	✅

表格中☑表示該防空系統攔截該空中威脅；❌表示該空中威脅突穿該防空攔截系統，或者攔截失敗。

資料來源：生成式 AI（Microsoft Copilot）生成。

由表 3 可以瞭解空中威脅極音速飛彈——法塔（T_1）由薩德和鐵穹系統雙重攔截，可以符合多重攔截的條件。空中威脅飛彈——柯蘭沙爾飛彈-4（T_2）由箭式加大衛投石索接戰，增加其攔截率。空中威脅無人機——見證者 129（T_3）由大衛投石索和鐵穹雙重攔截，屬於中低空層威脅，這樣的配置屬於合理。

二、防空飛彈成本來考慮多層次防禦效應

鑑於上述分析，接下來將分成兩個階段，進一步在防空飛彈成本條件下去探討多層次攔截效應。第一個階段，考慮防空飛彈系統的成本，將檢視該模型會呈現什麼結果？在考慮防空飛彈系統的成本，此時整理不同防空飛彈系統每枚成本如表 4 以及適用威脅類型。

表 4、防空飛彈系統每枚成本

防空飛彈系統	攔截每枚成本（仟美元）	適用威脅類型
薩德	約$12,000~$15,000[6]	法塔、柯蘭沙爾飛彈-4
箭式	約$2,500[7]	法塔、柯蘭沙爾飛彈-4

[6] 張威翔，〈12 天打掉 355 億！美軍援以色列消耗大量庫存 每月產量僅 8 枚〉，《中時新聞網》，2025 年 6 月 27 日，https://www.chinatimes.com/ realtimenews/20250627000058-260417?chdtv。

[7] 〈以色列整體防空系統評析暨借鏡〉，《思想坦克》，2025 年 6 月 4 日，https://voicettank.org/20250604-2/。

大衛投石索	約$1,000[8]	柯蘭沙爾飛彈-4、見證者129
鐵穹	約$50[9]	見證者 129

資料來源：作者自行整理。

此時多層次防禦配置基於表 4 的條件下，整理為表 5。

表 5、多層次防禦攔截配置建議

空中威脅	初層攔截系統	備援層攔截系統
法塔	箭式	薩德
柯蘭沙爾飛彈-4	大衛投石索	箭式或薩德(視預算與威脅強度)
見證者 129	鐵穹	大衛投石索

資料來源：作者自行整理。

依據表 5 在考慮攔截飛彈每枚成本與飛彈攔截成功率，轉成風險成本如方程式（5）

風險成本＝攔截飛彈每枚成本*（1-攔截成功率）（5）

在方程式（5）使用生成式 AI（Microsoft Copilot）將 QUBO 轉換為矩陣形式去求解，重新獲得如下的結果如表 6（成本最小）與表 7（攔截率最大）。

表 6、模擬退火器得到的最佳解（成本最小攔截率）

防空系統/威脅	法塔	柯蘭沙爾飛彈-4	見證者 129
薩德	☑	❌	❌
箭式	❌	☑	❌
大衛投石索	❌	☑	☑
鐵穹	☑	❌	☑

表格中☑表示該防空系統攔截該空中威脅；❌表示該空中威脅突穿該防空攔截系統，或者攔截失敗。

資料來源：生成式 AI（Microsoft Copilot）生成。

表 6 所呈現的結果大抵與表 5 多層次防禦攔截配置建議相似，唯一最大的差異在於法塔威脅，原先戰術的建議初層攔截是由箭式

[8] Yuval Azulay, "From Arrow to Iron Dome: The economics of Israel's Air Defense Strategy," *CTECH*, April 15, 2024. https://www.calcalistech.com/ctechnews/article/h18og9cl0#google_vignette.

[9] 同註 7。

負責，因為成本較低，備援再由薩德負責；但是模擬退火器法塔威脅竟是由薩德與鐵穹攔截，因為鐵穹並不適合攔截極音速彈道飛彈。模擬退火器完全是根據 QUBO 模型中的「數學目標函數」來尋找最低能量解，它不具備戰術常識，而是依據限制條件（每個威脅至少被攔截一次）與成本條件，因此才會產出模型與戰術之間的落差。

參、趨勢研判

一、飽和攻擊下的有效防禦

此次伊朗對以色列中高強度的飽和攻擊，依據參考資料瞭解 12 天期間美軍援助以色列就消耗 15 至 20 枚的「薩德」（THAAD）末段高空區域防禦系統飛彈庫存量。[10]因此，值得思考便是如何在有限資源的情況下，建構最合適的多層防禦架構。以色列的防空系統對於不同空域防禦的整合較為完整，由上述說明便可以瞭解。惟文章中沒有指出防空系統該如何部署在政府機關、民生設施（包含水、電、油與通訊）甚至於軍事關鍵設施（機場、船廠與船艦港口、油庫）。所以如何在高價值目標與民生設施之間去做取捨？生成式 AI（Microsoft Copilot）建議將威脅優先順序與目標價值去做割捨，例如：高價值目標（如政府機關、軍事關鍵設施）就應該部署防禦功能較高的防空飛彈系統，然而民生設施則建議可以採用單枚成本較低，迅速反應的系統較適宜。

二、混和攻擊下的成本考量

本文討論的空中威脅包含法塔、 柯蘭沙爾飛彈-4、 以及無人機見證者 129 成本整理成表 7。

[10] "U.S. Used Up 15-20 Percent of its Global THAAD Anti-Missile Arsenal in Just 11 Days of Mid-Intensity Combat: Cost Over $800 Million," *Force Index*, June 25, 2025, https://reurl.cc/EQnARv.

表 7、來襲威脅每枚成本

威脅系統	類型	單位成本（估算）	備考
法塔	極音速飛彈	$10 萬美元[11]	
柯蘭沙爾飛彈-4	中長程彈道飛彈	約$8 百萬美元[12]	
見證者 129	長航時無人機	約$375-[13]5,000[14]仟美元	依據開發成本、生產成本與元件成本(感測器、光學儀器與導航系統)，因此價格會產生差異。

資料來源：生成式 AI（Microsoft Copilot）生成，並由作者加以確認。

因此在不同成本的條件下，如何利用低成本的空中威脅去造成對方防空武器反制的飽和，伊朗派遣數百架無人機與百枚飛彈進行報復，如此高低配的混和攻擊，不僅造成以色列防空飛彈迅速的消耗，同時突穿其多層次的防空網，造成其關鍵基礎設施損壞以及人員的傷亡。所以如何在混和攻擊條件下，從成本的考量，做最有效的反制方式。對於伊朗派遣百架無人機，以色列則派遣戰機前往接戰，以企圖其在抵達以色列境內就被擊落。[15]如此做法也可以減輕其防空飛彈系統的負荷。

對比於以色列，我國的多重空間領域的防禦體系也有各自負責的防空系統，例如：天弓系統、愛國者系統、國家先進地對空飛彈

[11] "Unveiling the Fattah-2 Missiles: Iran's $20 Million Attack on Israel Demonstrates Enhanced Military Strength," *LBC*, March 10, 2024, https://reurl.cc/Om0OG7.

[12] Arezoo Karimi, "Iran Missile Strikes Cost Billions of Dollars in 12-Day War," *IRANWIRE*, June 29, 2025, https://iranwire.com/en/economy/142803-iran-missile-strikes-cost-billions-of-dollars-in-12-day-war/.

[13] Eric Tegler, "$375,000 - The Sticker Price For An Iranian Shahed Drone," *Forbes*, February 7, 2024, https://www.forbes.com/sites/erictegler/2024/02/07/375000the-sticker-price-for-an-iranian-shahed-drone/.

[14] Melvin Stanley, "The Hidden Cost of Iranian Drones: What's the Real Price Tag?" *NextTools*, https://nexttools.net/how-much-do-the-iranian-drones-cost/.

[15] 陳玫穎，〈【有片】以色列出動 200 架戰機猛轟伊朗　伊朗無人機已抵伊拉克上空〉，《上報》，2025 年 6 月 13 日，https://www.upmedia.mg/ news_info.php?Type=3&SerialNo=232536。

系統（National Advanced Surface-to-Air Missile System, NASAMS）、陸射劍二系統、復仇者防空系統。鑑於以上的說明，無論是飽和攻擊亦或者是混和攻擊，透過擊殺鏈（kill chain）從偵察敵方威脅到接戰包含以下六項步驟：發現（Find）、鎖定（Fix）、追蹤（Track）、標定（Target）、接戰（Engage）、評估（Assess），希望能夠引進 AI（甚至未來採用量子電腦）快速計算做各種武器系統有效率的分配與部署，以期達到攔截率最高、攔截效率最好、關鍵設施損壞最少的境界。

發行人 / 霍守業
總編輯 / 劉峯瑜
主任編輯 / 洪子傑 執行主編 / 方琮嬿
助理編輯 / 舒孝煌、許智翔、洪銘德、林柏州、鄧巧琳、
周若敏